RSAC 2025 Conference

Many Voices.
One Community.

SESSION ID: PART4-R03

Introducing a New "Kill Chain" Taxonomy for Combating Retail Fraud

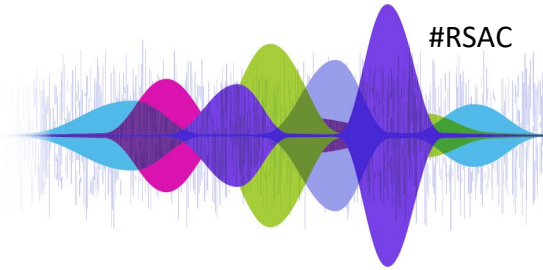
Christian Beckner

Executive Director, Center for Digital Risk & Innovation
VP, Retail Technology & Cybersecurity, National Retail Federation
www.linkedin.com/in/christianbeckner

Evan Gaustad

Senior Director, Threat Detection, Fraud & Abuse
Target Corporation
www.linkedin.com/in/evangaustad

Disclaimer



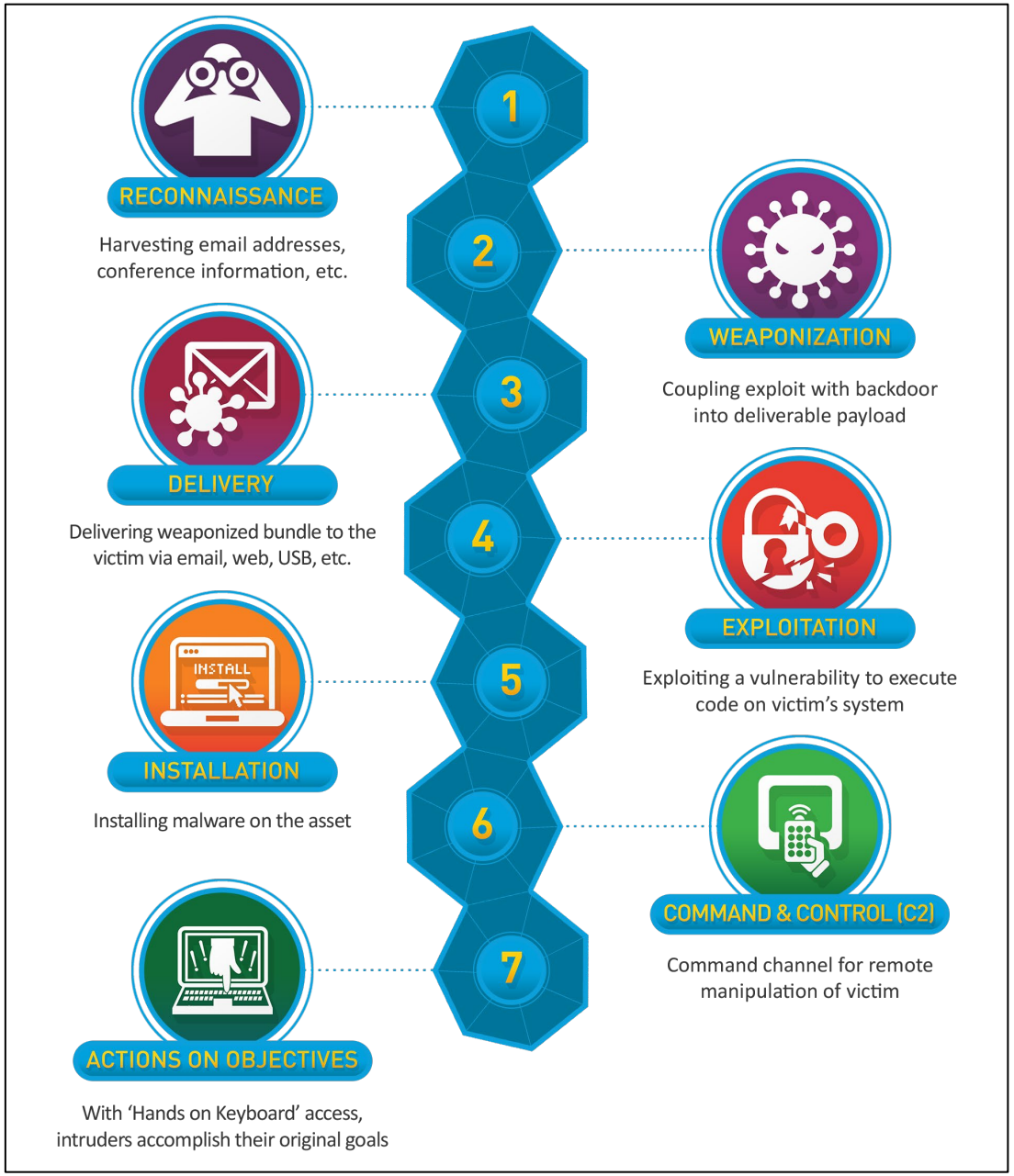
Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference LLC does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

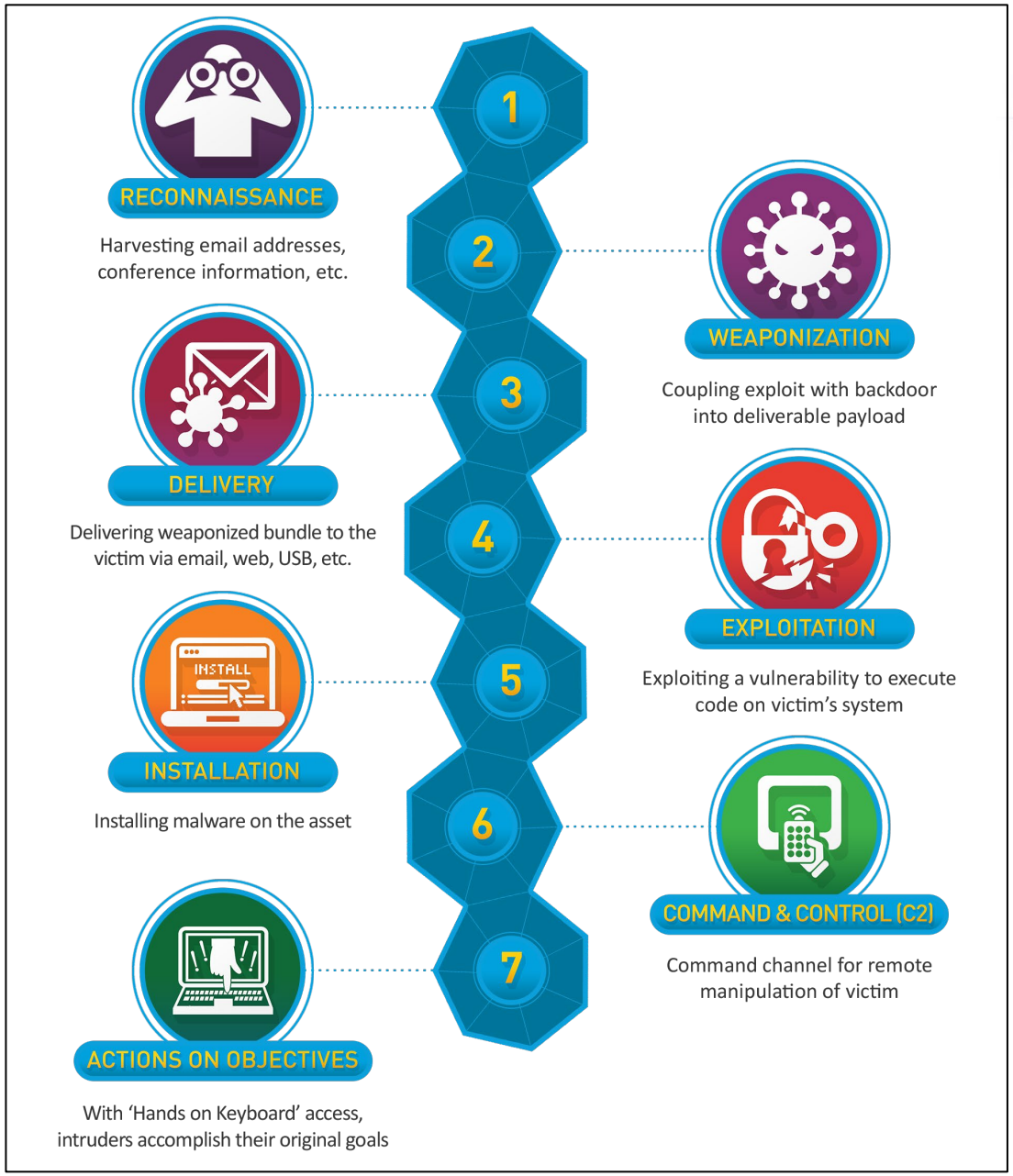
© 2025 RSA Conference LLC or its affiliates. The RSAC and RSAC CONFERENCE logos and other trademarks are proprietary. All rights reserved.

15 years ago…

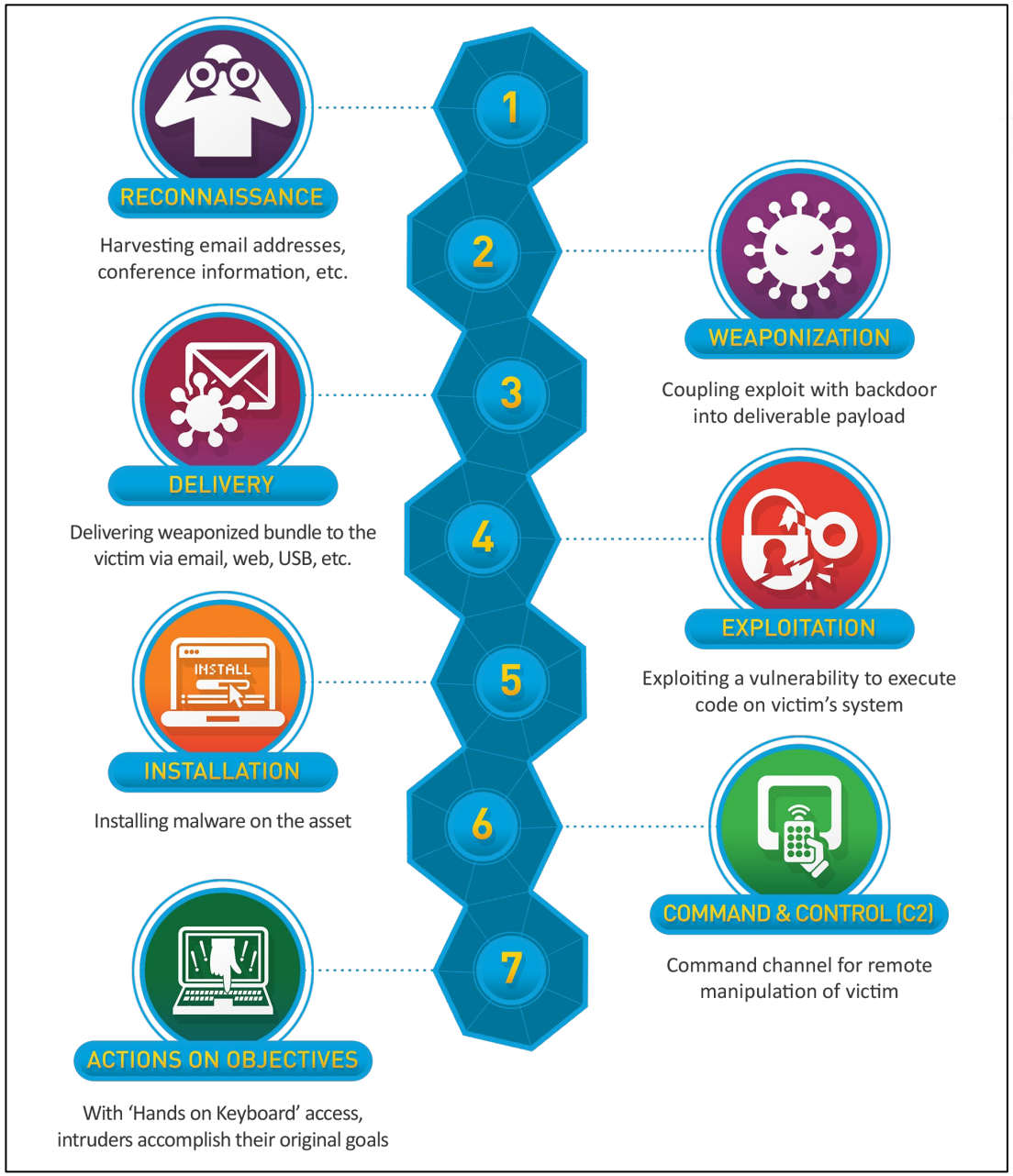
- Cybercriminals became more specialized
  - Malware sale and operators
  - Buying and selling stolen data
  - Vulnerability and exploit sale
  - Cybercrime and nation state-sponsored actors commonly known in industry

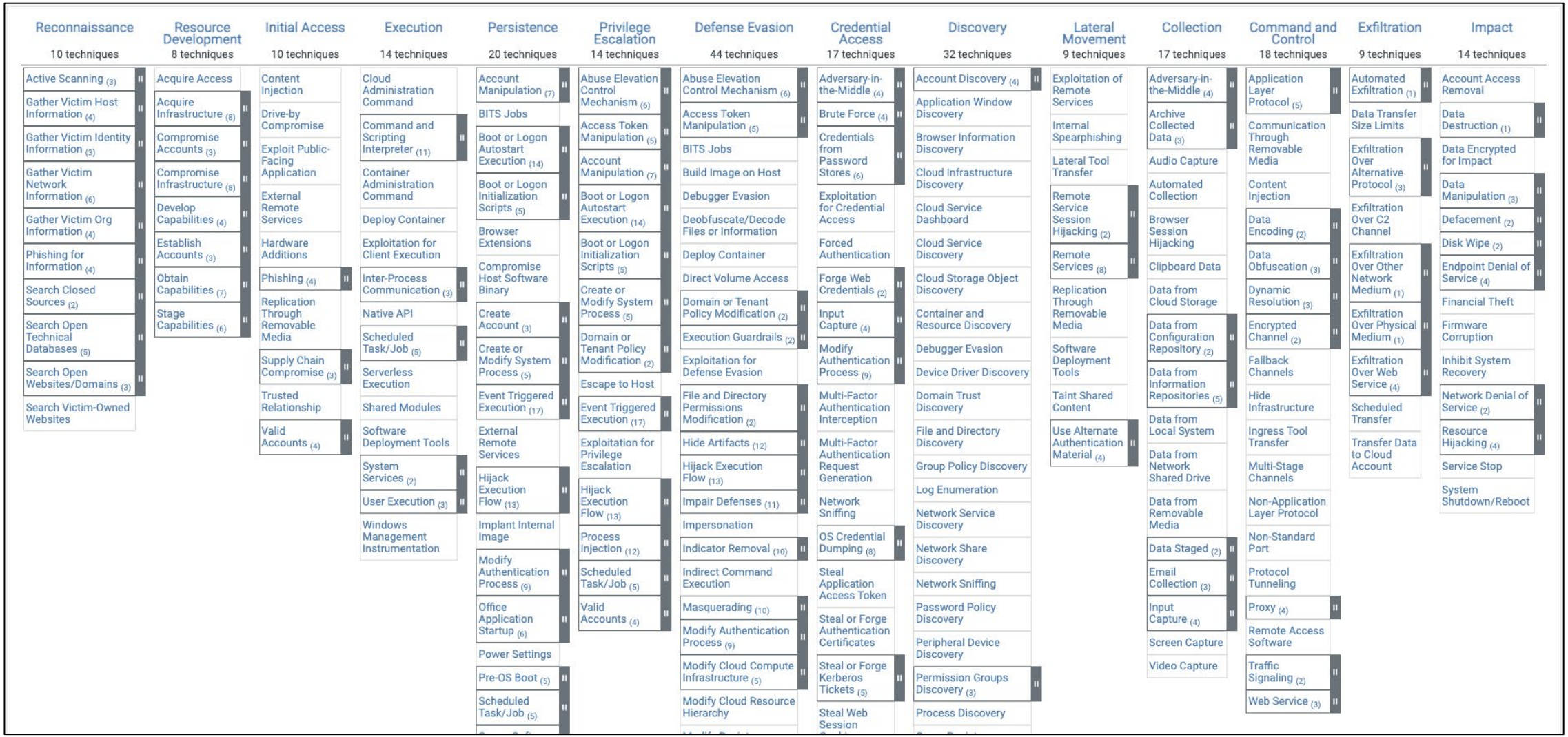

1
RECONNAISSANCE
Harvesting email addresses, conference information, etc.
2
WEAPONIZATION
Coupling exploit with backdoor into deliverable payload
3
DELIVERY
Delivering weaponized bundle to the victim via email, web, USB, etc.
4
EXPLOITATION
Exploiting a vulnerability to execute code on victim's system
5
INSTALL
INSTALLATION
Installing malware on the asset
6
COMMAND & CONTROL (C2)
Command channel for remote manipulation of victim
7
ACTIONS ON OBJECTIVES
With 'Hands on Keyboard' access, intruders accomplish their original goals

Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains, 2011



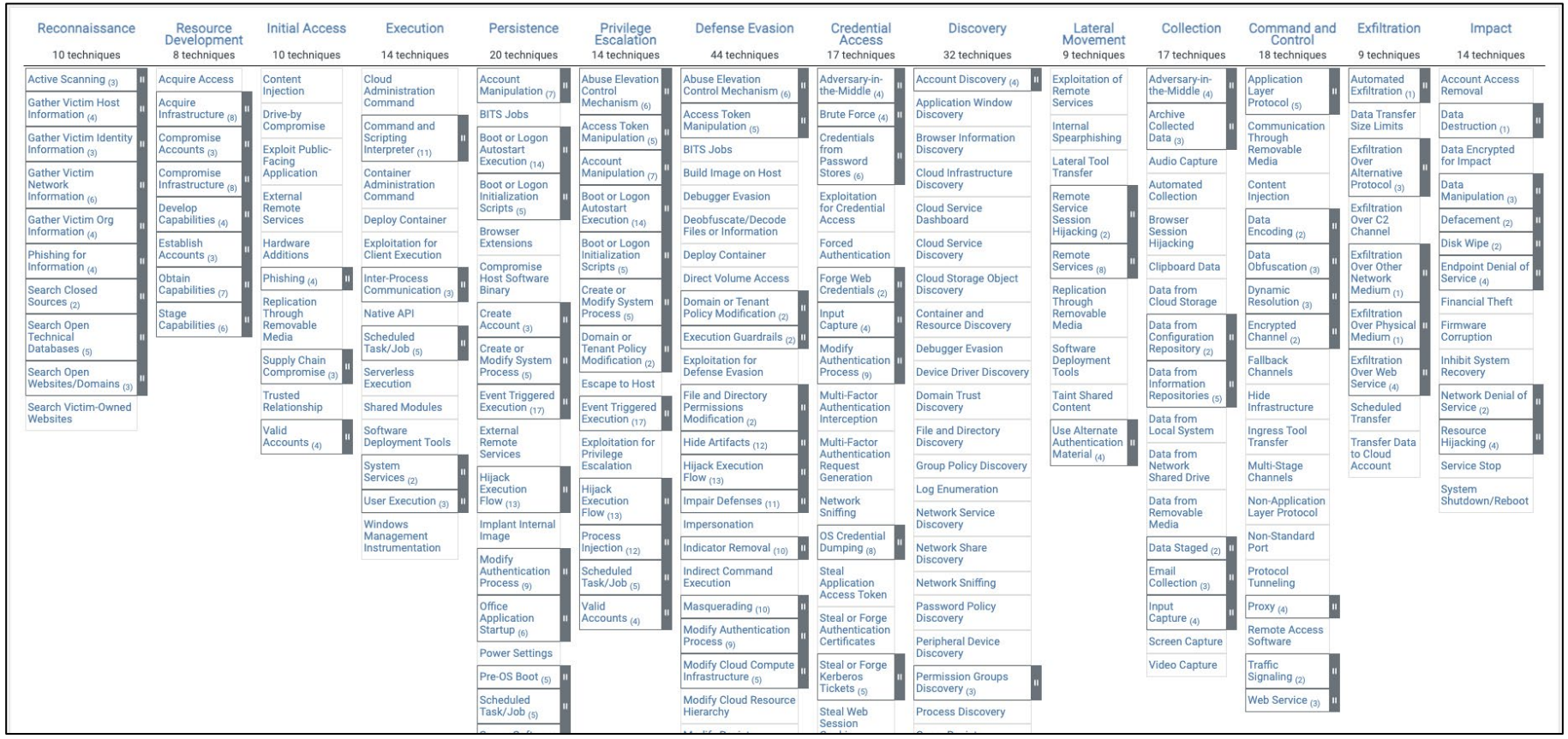
Recognition threat actors go through a multi-step process to complete their objectives



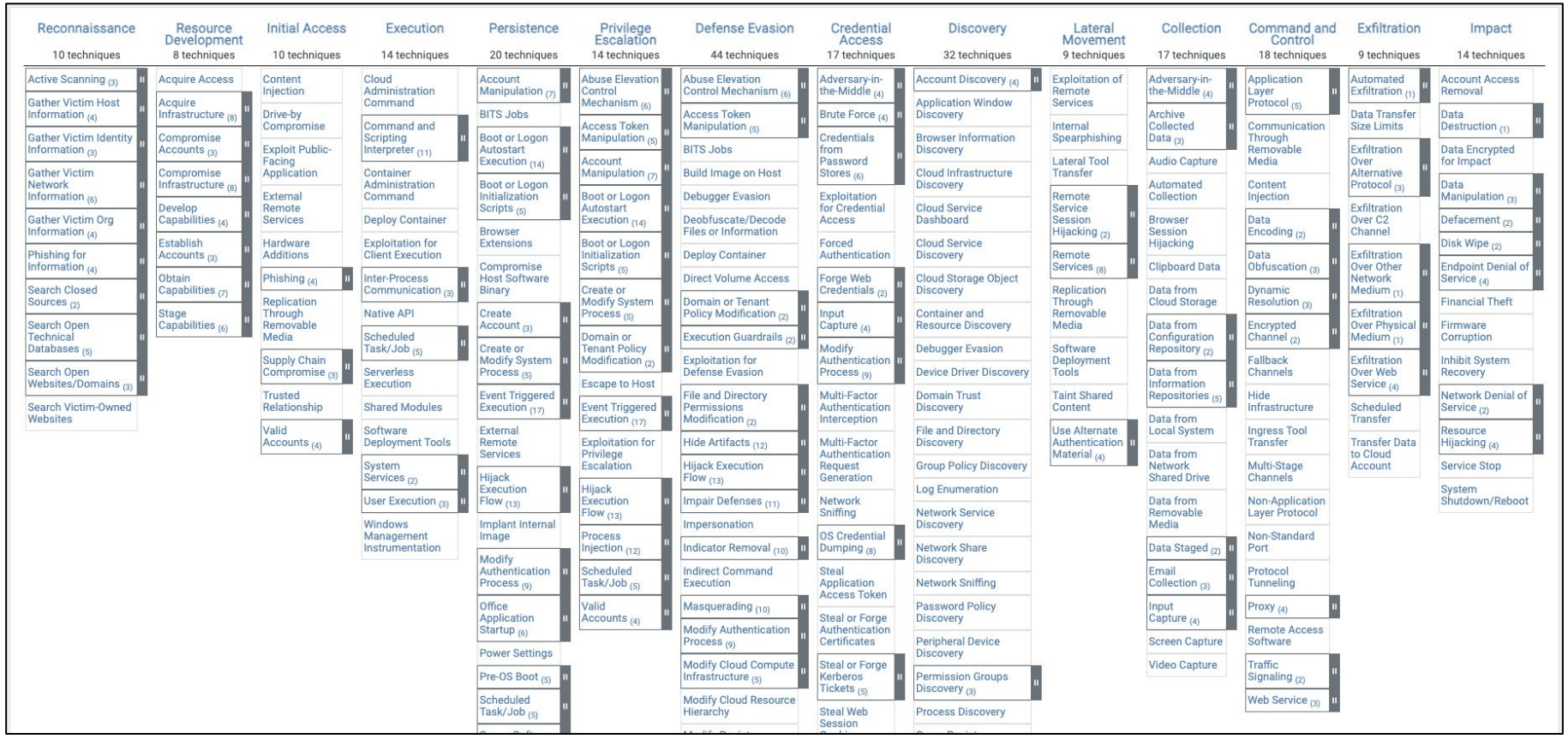


Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
10 techniques	8 techniques	10 techniques	14 techniques	20 techniques	14 techniques	44 techniques	17 techniques	32 techniques	9 techniques	17 techniques	18 techniques	9 techniques	14 techniques
Active Scanning (3)	Acquire Access	Content Injection	Cloud Administration Command	Account Manipulation (7)	Abuse Elevation Control Mechanism (6)	Abuse Elevation Control Mechanism (6)	Adversary-in-the-Middle (4)	Account Discovery (4)	Exploitation of Remote Services	Adversary-in-the-Middle (4)	Application Layer Protocol (5)	Automated Exfiltration (1)	Account Access Removal
Gather Victim Host Information (4)	Acquire Infrastructure (8)	Drive-by Compromise	Command and Scripting Interpreter (11)	BITS Jobs	Access Token Manipulation (5)	Access Token Manipulation (5)	Brute Force (4)	Application Window Discovery	Internal Spearphishing	Archive Collected Data (3)	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction (1)
Gather Victim Identity Information (3)	Compromise Accounts (3)	Exploit Public-Facing Application	Container Administration Command	Boot or Logon Autostart Execution (14)	Account Manipulation (7)	BITS Jobs	Credentials from Password Stores (6)	Browser Information Discovery	Lateral Tool Transfer	Audio Capture	Content Injection	Exfiltration Over Alternative Protocol (3)	Data Encrypted for Impact
Gather Victim Network Information (6)	Compromise Infrastructure (8)	External Remote Services	Deploy Container	Boot or Logon Initialization Scripts (5)	Boot or Logon Autostart Execution (14)	Build Image on Host	Exploitation for Credential Access	Cloud Infrastructure Discovery	Remote Service Session Hijacking (2)	Automated Collection	Data Encoding (2)	Exfiltration Over C2 Channel	Data Manipulation (3)
Gather Victim Org Information (4)	Develop Capabilities (4)	Hardware Additions	Exploitation for Client Execution	Browser Extensions	Boot or Logon Initialization Scripts (5)	Debugger Evasion	Forced Authentication	Cloud Service Dashboard	Remote Services (8)	Browser Session Hijacking	Data Obfuscation (3)	Exfiltration Over Other Network Medium (1)	Defacement (2)
Phishing for Information (4)	Establish Accounts (3)	Phishing (4)	Inter-Process Communication (3)	Compromise Host Software Binary	Create or Modify System Process (5)	Deobfuscate/Decode Files or Information	Forge Web Credentials (2)	Cloud Service Discovery	Replication Through Removable Media	Clipboard Data	Dynamic Resolution (3)	Exfiltration Over Physical Medium (1)	Disk Wipe (2)
Search Closed Sources (2)	Obtain Capabilities (7)	Replication Through Removable Media	Native API	Create Account (3)	Domain or Tenant Policy Modification (2)	Deploy Container	Input Capture (4)	Cloud Storage Object Discovery	Software Deployment Tools	Data from Cloud Storage	Encrypted Channel (2)	Exfiltration Over Web Service (4)	Endpoint Denial of Service (4)
Search Open Technical Databases (5)	Stage Capabilities (6)	Supply Chain Compromise (3)	Scheduled Task/Job (5)	Create or Modify System Process (5)	Domain or Tenant Policy Modification (2)	Direct Volume Access	Modify Authentication Process (9)	Container and Resource Discovery	Taint Shared Content	Data from Configuration Repository (2)	Fallback Channels	Scheduled Transfer	Financial Theft
Search Open Websites/Domains (3)		Trusted Relationship	Serverless Execution	Event Triggered Execution (17)	Escape to Host	Domain or Tenant Policy Modification (2)	Multi-Factor Authentication Interception	Debugger Evasion	Use Alternate Authentication Material (4)	Data from Information Repositories (5)	Hide Infrastructure	Transfer Data to Cloud Account	Firmware Corruption
Search Victim-Owned Websites		Valid Accounts (4)	Shared Modules	External Remote Services	Event Triggered Execution (17)	Execution Guardrails (2)	Multi-Factor Authentication Request Generation	Device Driver Discovery		Data from Local System	Ingress Tool Transfer		Inhibit System Recovery
			Software Deployment Tools	Hijack Execution Flow (13)	Exploitation for Privilege Escalation	Exploitation for Defense Evasion	Network Sniffing	Domain Trust Discovery		Data from Network Shared Drive	Multi-Stage Channels		Network Denial of Service (2)
			System Services (2)	Implant Internal Image	Hijack Execution Flow (13)	File and Directory Permissions Modification (2)	OS Credential Dumping (8)	File and Directory Discovery		Data from Removable Media	Non-Application Layer Protocol		Resource Hijacking (4)
			User Execution (3)	Modify Authentication Process (9)	Process Injection (12)	Hide Artifacts (12)	Steal Application Access Token	Group Policy Discovery		Data Staged (2)	Non-Standard Port		Service Stop
			Windows Management Instrumentation	Office Application Startup (6)	Scheduled Task/Job (5)	Hijack Execution Flow (13)	Steal or Forge Authentication Certificates	Log Enumeration		Email Collection (3)	Protocol Tunneling		System Shutdown/Reboot
				Power Settings	Valid Accounts (4)	Impair Defenses (11)	Steal or Forge Kerberos Tickets (5)	Network Service Discovery		Input Capture (4)	Proxy (4)		
				Pre-OS Boot (5)		Impersonation	Steal Web Session	Network Share Discovery		Screen Capture	Remote Access Software		
				Scheduled Task/Job (5)		Indicator Removal (10)		Network Sniffing		Video Capture	Traffic Signaling (2)		
						Indirect Command Execution		Password Policy Discovery			Web Service (3)		
						Masquerading (10)		Peripheral Device Discovery					
						Modify Authentication Process (9)		Permission Groups Discovery (3)					
						Modify Cloud Compute Infrastructure (5)		Process Discovery					
						Modify Cloud Resource Hierarchy							

MITRE ATT&CK Enterprise, 2013



Cataloged techniques used by threat actors and steps defenders can take to defend themselves



Risk Context: Increasing Impact of Retail Fraud Threats

Retailer Impact

- Total cost of ecommerce fraud to merchants expected to rise from $44.3 billion in 2024 to $107 billion in 2029 (Juniper Research)

Consumer Impact

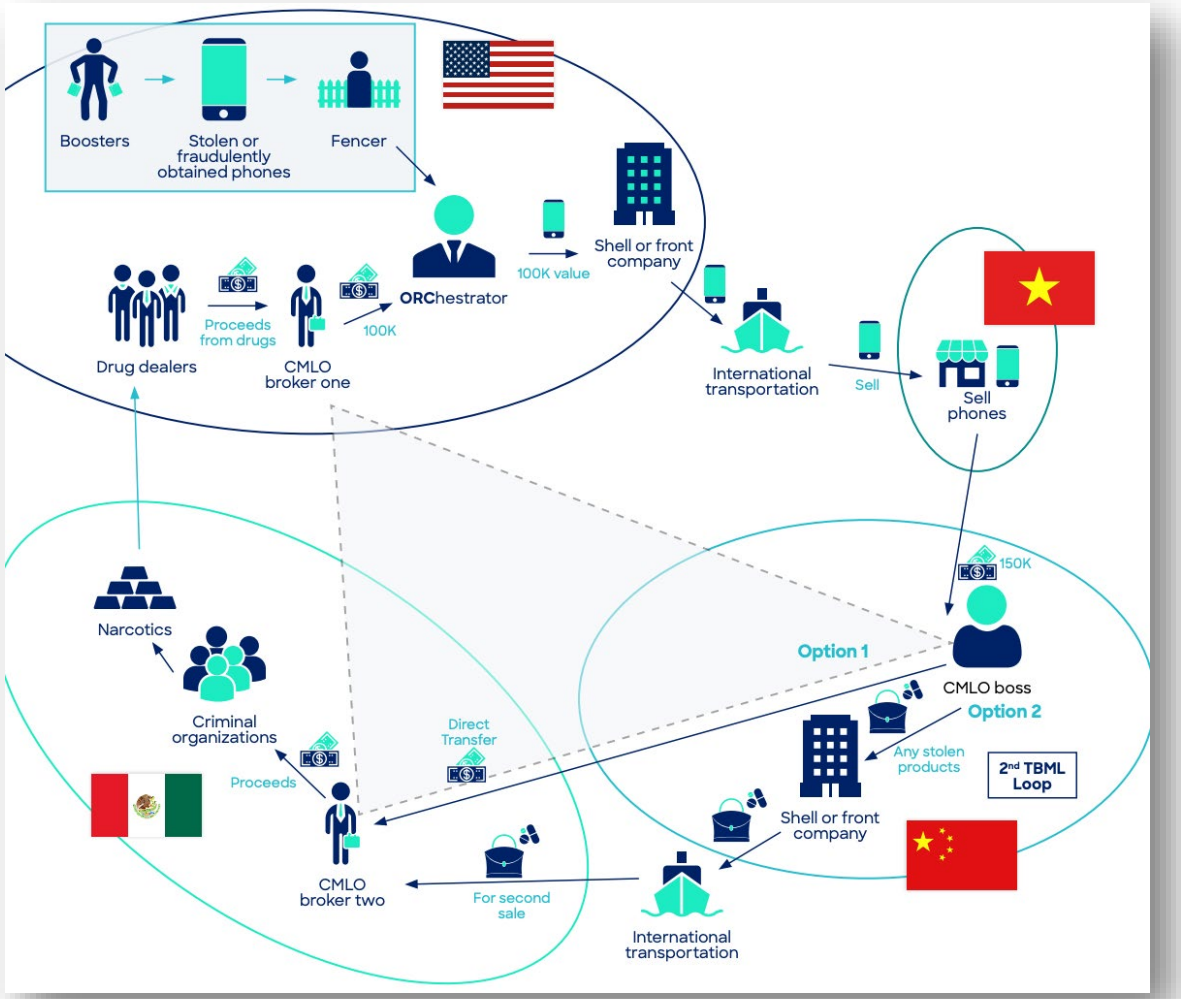
- 29% of U.S. population have experienced account takeover in 2023, up from 22% in 2021 (security.org)
- Effects: financial, emotional and safety

National Security Impact

- Funds international organized crime – facilitates money laundering of organized crime groups involved in fentanyl and human trafficking

Organized Retail Crime Scale and Complexity

- ORC crosses state and international borders
- Multiple hierarchical and specialized groups and actors
- New and traditional intermingled criminal activities



Source: 2022, ACAMS & HSI, Detecting and Reporting the Illicit Financial Flows Tied to Organized Theft Groups (OTG) and Organized Retail Crime (ORC)

What is the Retail Fraud Taxonomy?

- Knowledge-base of fraud techniques derived from real-world observations.
  - Sourcing: wide range of retail fraud professionals.
  - Purpose: education, communication, security assessments, team exercises, and resource prioritization.

Use Cases – How Practitioners Can Use Taxonomy

- **Security Architecting**
- **Business Case Justification**
- **Testing**
- **Information sharing**
- **Vendor Evaluation**

Structure

	Term	Description
1	**Tactics**	• Fraudster's step-wise objectives or goals during each phase of a scheme.
2	**Techniques**	• The various methods a Fraudster's will use to support a tactic.
3	**Mitigations**	• Security concepts and technologies to prevent or disrupt technique from being successfully executed.
4	**Detection Sources**	• Telemetry that can be collected to detect fraud.
5	**Schemes**	• Objective of fraud activity, which can be broken down into a series of Tactics, Techniques and Procedures (TTPs).
6	**References**	• Academic Research, Case studies, Threat Intelligence, Security Blogs, etc. that are used to inform taxonomy.

Technique Example Overview

Check Gift Card Balance FT1103
Tactics: Initial Access
Schemes: Gift Card Fraud
Sub Techniques: Application FT1103.1, Phone Verification FT1103.2
Description: The Fraudster may abuse legitimate functions to confirm a Gift Card is active and has funds. To reduce overhead retailers may have autonomous systems for gift card owners and recipients to check if their gift card is usable and has value. These systems are generally available to the public for interaction.

- **Mitigation**
  - Login Required
    - Require authentication before displaying gift card status or value
  - Access Code required
    - Require an access code that is separate from the Gift Card number before revealing the status and funds on the gift cards
  - Online Location Data
    - Some physical locations should not be able to check Gift Card Balance. Some locations may also be the source of repeated fraud attempts. Prevent the ability to check gift card status and funds based on locations.
  - Phone Number
    - Automatically block phone numbers related to VoIP services and phone numbers that have been known to be perpetrate fraud
- **Detection**
  - Network Traffic Attributes
    - Monitor for the Network Traffic Attributes such as IP Address, DNS Name, ASN, and other digital location attributes especially if some of these sources have known fraud activity or has a high risk of fraud activity
  - Time Based Attributes
    - Based on the location of your operations, monitor for activities that occur during off hours.
  - Device Attributes
    - Monitor device factors such as device type, user agent string, operating system, cookies
- **References**
  - Industry Partner Collaboration

Technique entries will each display:

- Tactic
- Scheme
- Sub technique (if applicable)
- Technique Description
- Mitigations
- Detections
- References

Mitigation Example Overview

Login Required MT1002

Description

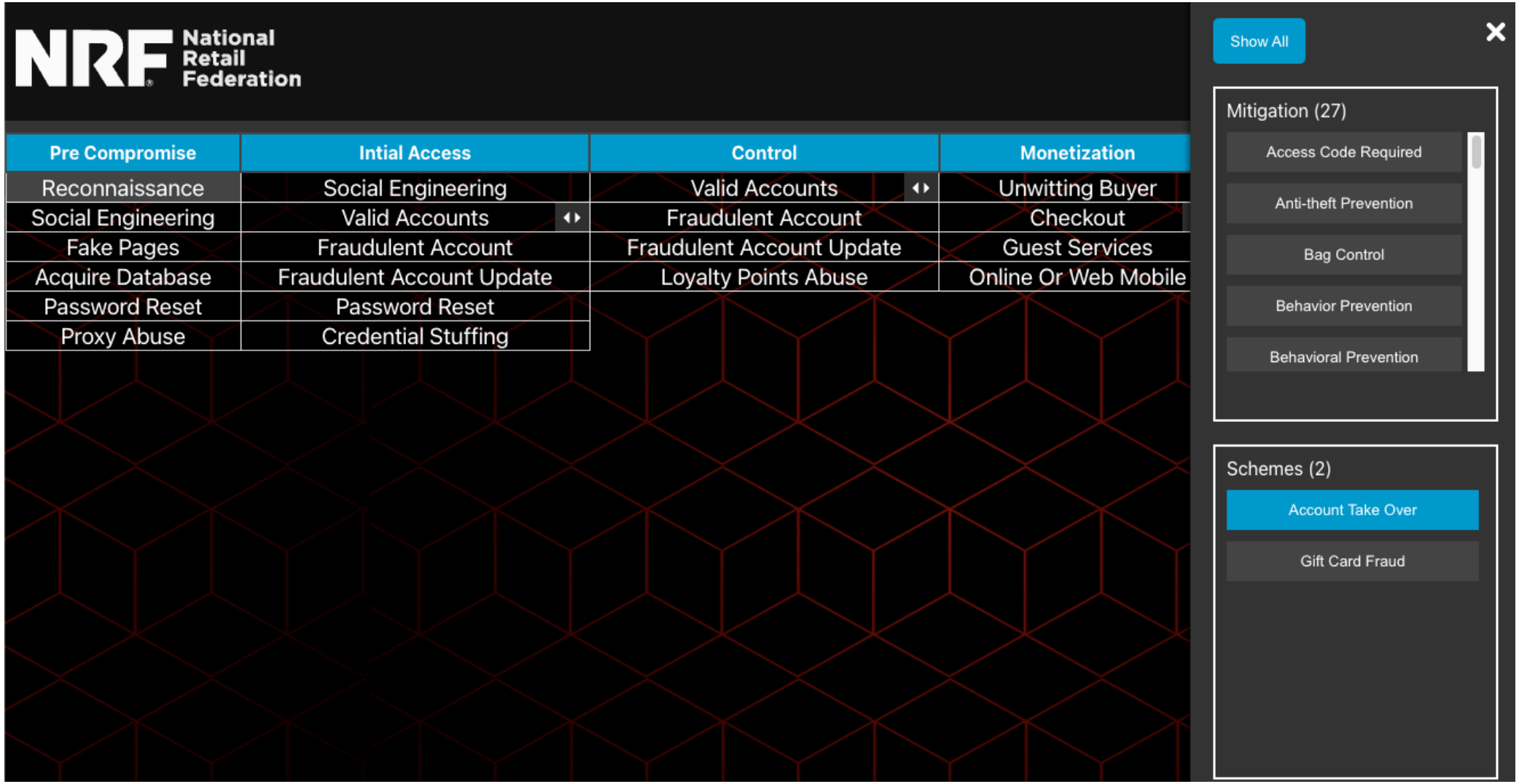
- Ensure a Gift Card is tied to an authentication source before allowing activation, use or transfer

Technique(s) Mitigated

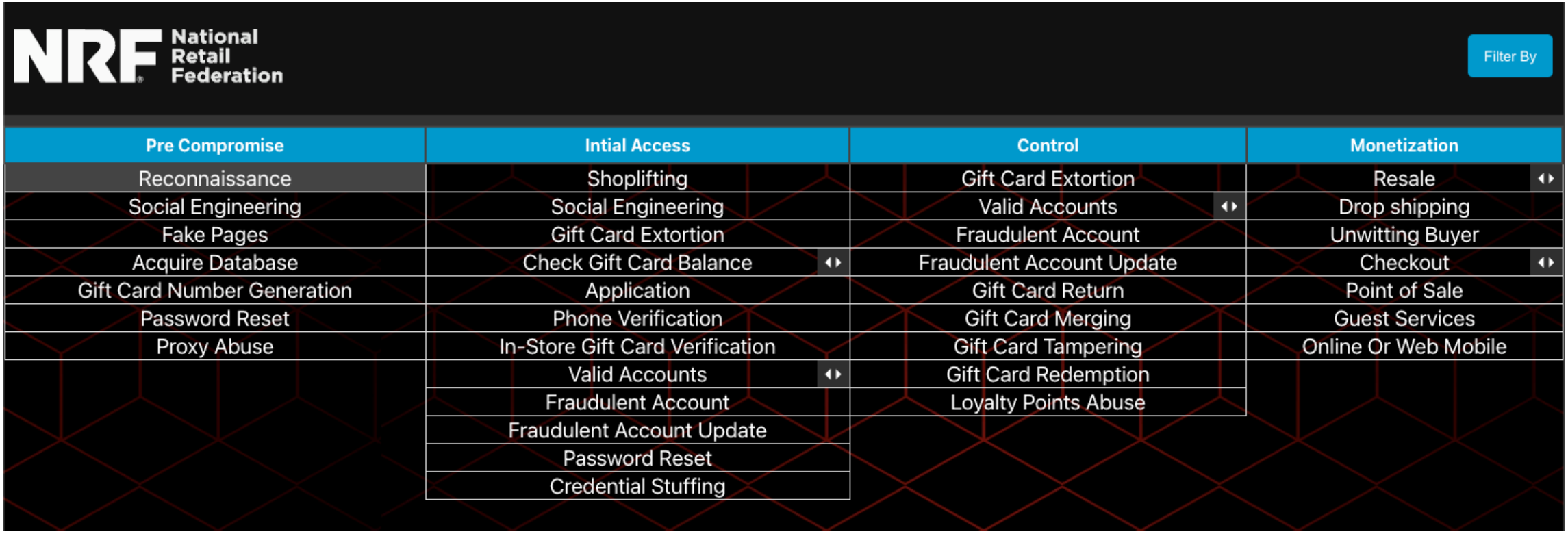
- Gift Card
- Extortion
- Check Gift Card Balance
- Check Gift Card Balance: Application
- Gift Card Control
- Gift Card Merge
- Resale
- Drop Shipping
- Gift Card Purchase

- Mitigation entries have a short description and a link to all techniques mitigated.
- Using this view, you can see additional threat techniques that this mitigation can disrupt.
- This view can be used to identify mitigations providing the most value.

Web application view: schemes & mitigations



Apply: Live Taxonomy Web Application

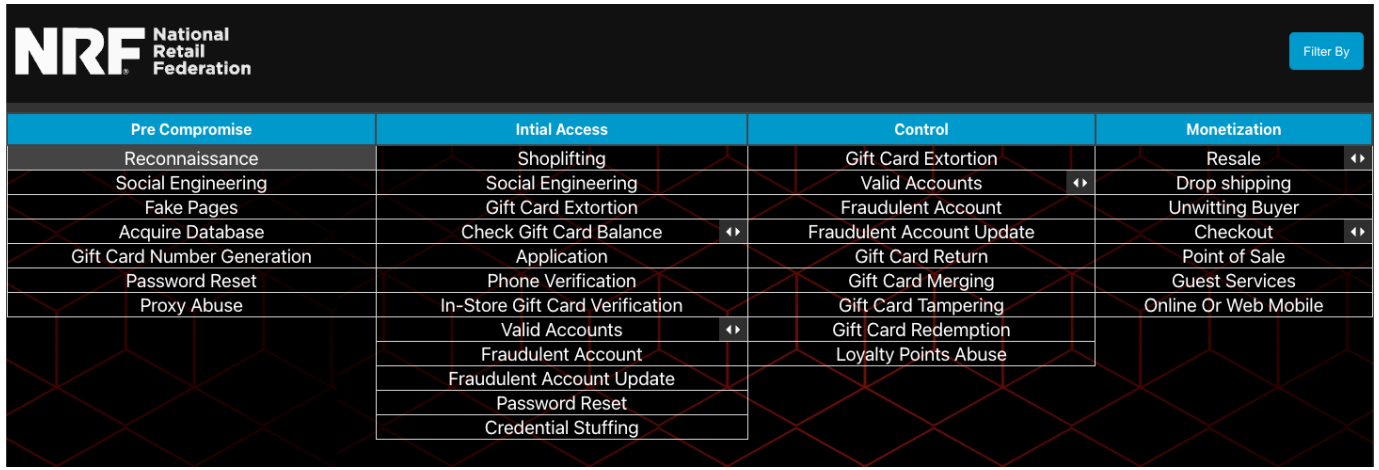


Available here: https://target.github.io/retail-fraud-taxonomy-viewer/

Apply: Live Taxonomy Web Application

Try it!

- Incorporate into business risk assessments
- Assess detection and control coverage
- Introduce the vocabulary & definitions to your teams



Available here: https://target.github.io/retail-fraud-taxonomy-viewer/

Future State

Dynamic and continuously evolving resource – contribute!

- **Knowledge-base inputs (threat drivers)**
- **Knowledge-based outputs (techniques, mitigations, etc.)**
- **Language of fraud professionals**
- **Sharing**
- **User feedback**

Collaborate

Led & Sponsored by: NRF

In Cooperation with: RETAIL & HOSPITALITY ISAC; Retail Industry Members

Technical Advisor and Project Manager: TheChertoffGroup

For input, questions, please reach out to:

Christian Beckner: becknerc@nrf.com
Jon Tran: jon.tran@chertoffgroup.com

More information available here: https://nrf.com/research/retail-fraud-taxonomy

RSAC™ 2025 Conference

Many Voices.
One Community.

Thank You!